REMARKS

Independent claims 2 and 18 have been amended to include the features of claim 15 and claim 15 has been canceled. Claims 3 and 10 have been amended to provide clearer antecedent basis to amended claim 1, and claims 19 and 20 have been amended to provide clearer antecedent basis to amended claim 18. No new matter has been entered. Upon entry of the above amendments, claims 2-14 and 16-21 will remain in the application.

Objection to the Title

The Examiner requested a more descriptive title of the invention. Applicant has amended the title as proposed by the Examiner. Withdrawal of the objection to the title of the invention is solicited.

Claim Rejections – 35 U.S.C. §102(b)

Claims 2-21 stand finally rejected under 35 U.S.C. §102(b) as allegedly being anticipated by Rowland (US 6,405,318). Independent claims 1 and 18 have been amended to include the features of claim 15. Claims 1 and 18 as so amended are believed to be clearly differentiated from the teachings of Rowland. Withdrawal of the rejection of claims 2-21 as being anticipated by Rowland is respectfully requested for at least the reasons given below.

The claimed invention relates to a system and corresponding method for detecting the state of a computer network. As set forth in amended claim 2, the system includes:

agents disposed in said computer network, each said agent comprising:

data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network;

means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said network in a normal state and activities of said network in an abnormal state; and

means for comparing collected data to said activity models to determine the state of said computer network at different times and to dynamically update said activity models,

wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis to the results of pattern

matching by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network.

Claim 18 recites a corresponding method of detecting the state of a computer network. Such a system and method is not taught or suggested by Rowland.

Rowland discloses an intrusion detection system that monitors a computer system in real-time to identify activity indicative of attempted or actual access by unauthorized persons or computers. The occurrence of false alarms is purportedly reduced by comparing the user's behavior to the user's profile and known attack patterns and automatically taking action when an event (anomaly) is identified. The user's profile is dynamically updated during each use and saved. In the main embodiments, the intrusion detection system is implemented in software on a host computer. In the embodiment of Figure 9, the system further includes a central controller in a network that contains multiple host computers 151-153. Each host computer 151-153 includes the monitoring software and sends information about log auditing, login anomaly detection, etc. to the central controller for centralized auditing of events 154, data analysis 155, cross-correlation of intrusion activity throughout the network 156, and alerting the network system administrator 157 if anomalous activity is found. However, other than the paragraph at column 8, lines 8-23, Applicant can find no further detail regarding the operation of the embodiment of Figure 9.

In the Final Rejection, the Examiner rejected claim 15 (the features of which are now incorporated into independent claims 2 and 18) by alleging that Rowland teaches at column 2, lines 50-66, and column 5, lines 30-35, the features of claim 15. Applicant submits that the Examiner has read too much into these disclosures. All Rowland says at the indicated locations is that a local or system controller may log events (such as positive results of comparisons with known attack patterns or suspicious command entries), disable accounts and block access to the system, and that information transfer may be used to coordinate intrusion response. Applicant can find no teaching by Rowland of comparing pattern analysis results from different host systems in a computer network to "identify similar patterns of suspicious activity in different portions of the computer network" as claimed. Applicant submits that Rowland's general teaching of "coordinating information transfer" falls far short of suggesting identifying "similar patterns of suspicious activity in different portions of the

computer network" as claimed. If the Examiner disagrees, the Examiner is encouraged to indentify where Rowland suggests the network analysis now claimed. Applicant submits that the teachings of Rowland fall short of suggesting the claimed network level coordination of the detection of suspicious activities.

Withdrawal of the rejection of claims 2-14 and 16-21 as being anticipated by Rowland is thus proper and is respectfully solicited.

Conclusion

For the reasons set forth herein, the amendments to claims 2 and 18 are believed to place all claims in condition for allowance. A Notice of Allowability is solicited.

Date: Monday, May 12, 2008

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439